VLAN Zuweisung und WLAN Registrierung über Zertifikate bzw. Nutzername mit NPS RADIUS Windows Server

Inhaltsverzeichnis

- <u>1 Anlegen der Windowsgruppen</u>
- 2 Gruppenrichtlinien erstellen
- 3 NPS konfigurieren
- 4 Konfigurieren Unifi-Controller
- 5 Lan-fähige Windows Clients konfigurieren (bei Wifi-only Clients nicht nötig)
- 6 Ergebnis

Hallo zusammen.

Ich habe mir aus Folgendes eingerichtet. Es sorgt für Sicherheit und weniger Administrationsaufwand (kein neu Konfigurieren einzelner Switchports etc.). Ich will das hier mal für die Nachwelt festhalten (und damit ich es selbst wieder vergessen kann).

Was wollte ich erreichen?

1. Nutzer sollen sich mit ihrem AD-Nutzernamen am WLAN anmelden können.

2. Clients der Active-Directory sollen direkt in VLAN x verschoben werden, wenn sie sich im WLAN anmelden oder an einem Switch eingesteckt werden (Port unabhängig). Das geht ohne Nutzereingabe, sondern über Zertifikate.

3. nur noch eine SSID für alle VLANs (nur bedingt möglich, da hier die Clients mitspielen müssen. Z.B. unterstützen nicht alle IoT Geräte WPA2-Enterprise)

Voraussetzungen:

1. funktionierendes Active Directory (inkl. Benutzer/Computerverwaltung, sowie Gruppenrichtlinienverwaltung)

2. in AD registrierte Zertifizierungsstelle (Rolle unter Windows Server)

3. in AD registrierter NPS (Network Policy Server - deutsch: Netzwerkrichtlinienserver [Rolle unter Windows Server]) auch als RADIUS bekannt.

Wie ihr das alles trennt, ist letztendlich euer eigenes Ding, da es hier auf Sicherheit, Performance usw. ankommt.

Ich finde es immer schwierig, wo ich bei solchen Tutorials anfangen soll. Jedoch habe ich entschlossen, auf die grundlegende Einrichtung vom NPS und der CA zu verzichten. Hierzu gibt es genügend (gute) Tutorials im Netz. Ich gehe also davon aus, dass dies zum Zeitpunkt des Weiterlesens erfolgt und die Zusammenhänge verstanden sind.

Meine Infrastruktur sieht wie folgt aus. Das ist keine Vorgabe, ich zeige das nur, damit ihr die Namen der Server (falls relevant) bzw. die Rollenverteilung seht. Ich hoffe hiermit das ein oder andere Fragezeichen vermeiden zu können.

DC1: Active Directory Verwaltungsdienste. Für das Tutorial relevant sind nur die Benutzer/Computerverwaltung und die Gruppenrichtlinienverwaltung.

Util-01: allgemeiner Anwendungsserver. Hier läuft der NPS (Netzwerkrichtlinienserver).

CA-01: Certificat-Authority. Hier sind die AD-Zertifikatsdienste installiert.

Ich arbeite mit Windows Server 2019 und Windows 11 Clients.

Getestet habe ich das Ganze auch mit Win Server 2016 und Windows 10 Clients.

Laut Internet sollte die Prozedur ab Windows Server 2012 (R2?) und Windows 7 (Vista?) Clients funktionieren.

1 Anlegen der Windowsgruppen

AD Nutzer und Computerverwaltung öffnen und Gruppen anlegen, welche sich am RADIUS authentifizieren dürfen.

Grp-LanDevices (Alle AD Clients, welche sich per LAN verbinden, ihr müsst also Computer angeben, keine Benutzer)

Grp-WLanDevices (Alle AD Clients, welche sich per WLAN verbinden sollen, ihr müsst also Computer angeben, keine Benutzer)

Grp-WLAN-IoT (beinhaltet bei mir nur einen Nutzer, der für alle IoT Geräte verwendet wird, welche sich am WLAN anmelden)

Grp-WLAN-AD-Home (beinhaltet alle in AD angelegten Nutzer, welche sich mit ihrem Nutzernamen am WLAN anmelden können sollen)

2 Gruppenrichtlinien erstellen

Es gibt zwei GPOs, die ich für mein Vorhaben verwende.

Die GPO "Zertifikatsverteilung" ist für die automatische Zertifikatsverteilung verantwortlich. Sie wirkt auf alle Clients.

Die GPO "Wlan Profil" ist für die Verteilung des WLAN-Profils verantwortlich. Sie wirkt nur auf Clients, welche auch WLAN nutzen.

GPO "Zertifikatsverteilung"

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Richtlinien für öffentliche Schlüssel - Einstellungen der automatischen Zertifikatsanforderung

Rechtsklick - neu - Automatische Zertifikatsanforderung

Assistent durchklicken und "Computer" auswählen. Fertigstellen.

ubiquiti-networks-forum.de/attachment/15320/

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Richtlinien für öffentliche Schlüssel

Doppelklick "Zertifikatdienstclient - Automatische Registrierung". "Aktiviert" auswählen und beide Haken setzen.



GPO "Wlan Profil"

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Drahtlosnetzerkrichtlinien

Rechtsklick - "Erstellen Sie eine neue Drahtlosnetzwerkrichtlinie für Windows Vista und neuere Versionen"

Euere SSID anlegen. Wichtig: die Schreibweise muss identisch sein. Einstellungen entnehmt ihr bitte den Screenshots.

inggemichtliniemennaftungs-faitter		- 0	×
s Aktor Arakht 7			
Computation figuration	Name	Industry In	
Echtlerien	h dire	Register another bains Despects processing	
 Mindow-Einstellungen 		a new mean mean mean many a grange	
 Renemas/Resurgationile Science (Section and International) 			
> tele liweitgestellte Drucker			
Scherhotsenstellungen Montarichtlinken	Inte	llen Sie eine neue Drahtloanetzwerkrichtlinie fü	r Windows Vieta and severe Versioners.
> Galace Robellinien	Ene	neue Windows 82-Richtlinie-erstellen	
 a svegnaprotokoli bingeschnänkte Gruppen 	Although	alisieren	
> Systemilierate	Anal	det	
> 📮 Deteisystem	Speed	bole anordnan	
 III Richtlinien für Kabelnetzverke (2018 802.3) Winders Defender Firewall mit enweterter für 	Act I	laster ausrichten	
Networkister-Manager-Richtlinien Größerbereiterstellteiteren MMI MULTI-	1984		
 Richtlinien für affentliche Schlüssel 			
 Richtlinien f ür Softwareeinschstnlung Anwendungszteuerungsrichtlinien 			
IP-Sicherheitsrichtlinien auf Active Directory 8			
Concerns conversion de la construction de la constr	1		
		Eigenschaften von AD-Home	×
Algemein Netzwerkberechtigungen		Verbindung Sicherheit	
Die in dieser Richtlinie definierten Eigenschaften werden au	af alle	Pollower	
Drandosschnidsbelen der Clenicumputer angewendet.		AD-Home	
AD-Home		Networkname(n) (SSID):	
Autobas			Hrs.fign.
Wian für Lastron		AD-Home	Entlemen
The second second			
The Antomate Windows Wild Evolution does the Class	in unsandas		
Verbinden mit verflicharen Nettwerken in der Reihenhole	der unten		
aufgeisteten Profile:	and Grades	Netzwenktyp:	Zugiffspunit-basierend
Profinance SSID Authentifizie	Vers	P Asternatisch verbinden, wenn die	ses Netzwerk in Reichweite ist
AD-Home AD-Home WPA2-Enters	ABSI	Mit einers verfügbaren bevorzugte	en Netzwerk verbinden
	24	E Verbinden, selbst wenn das Netz	werk keine Kennung aussendet
	121		
	.4		
¢			
Hinzufügen Bearbeiten Endernen Importieren	Exportieren		OK Abbeshen
백9 AD-Home	Infra	struktur Zula	issen
Hinzufügen Entfe	rnen		
Verbindungen mit Ad-h	oc-Netzwe	erken verhindern	
- Terbindangen meral	oc nearro		
Verbindungen mit Infra	strukturne	tzwerken verhindern	
Anzeigen von abgelehr	nten Netzw	erken für Benutzer zu	ilassen
 Erstellen von Profilen fü 	ir alle Ben	utzer für jeden zulass	en
Gruppenrichtlinienprofi	le nur für z	ulässige Netzwerke v	erwenden
Dishtinionainstallungan	on Windo	ue 7 upd hähar	
Verschlüsselung:		AES-CCMP	-
Netzwerkauthentifizierur	ngsmethod	le auswählen:	
Microsoft: Smartcard-	oder ande	res Zertifikat 💌 🛽 🗄	Eigenschaften
Authentifizierungsmodu	s:		
Computerauthentifizie	rung	•	
Max. Authentifizierungs	ehler:	3	
Informationen für zu zwischenspeichem	künftige V	erbindungen mit diese	em Netzwerk

https://ubiquiti-networks-forum.de/wiki/entry/106-vlan-zuweisung-und-wlan-registrierung-%C3%BCber-zertifikate-bzw-nutzername-mit-npsra/ 4

1

Envoitert

3 NPS konfigurieren

Server-Manager - Tools - Netzwerkrichtlinienserver - Rechtsklick auf "NPS (lokal)" - Server in Active Directory registrieren (bei mir ausgegraut, da bereits erledigt)



Der Server, auf dem der NPS läuft, muss Mitglied der Gruppe "RAS- und IAS-Server" sein. Dann bezieht er automatisch ein Zertifikat von der Zertifizierungsstelle.

Anschließend Rechtsklick auf "RADIUS-Clients und -Server" - Neu

Hier legt ihr nun all eure Accesspoint und Switches an. Das ist eine Unifi-Eigenheit. andere Hersteller haben das eleganter gelöst und man muss nur den Controller anlegen. Daher kann es je nach Umfang eurer Infrastruktur einige Einträge geben. Beim Reiter "Erweitert" lasst ihr Standard im Drop-Down Menü stehen. Den "gemeinsamen Schlüssel" notiert ihr euch bitte, da dieser nach Eingabe nicht mehr angesehen werden kann. Ihr benötigt den nachher im inifi-Controller. Deswegen ist es auch zwingend nötig, bei allen angelegten Geräten im NPS den selben Schlüssel zu nehmen.

Als nächstes werden die Verbindungsanforderungsrichtlinie und die Netzwerkrichtlinie erstellt. Bei mir sind es 3 bzw. mit der Standard-Richtlinie eben dann 4.

Unterschieden habe ich in Nutzer, die ins interne Netz dürfen, IoT-Nutzer und den Sonderfall mit der Zertifikat-Authentifizierung. Die ersten drei Screenshots jeweils sind die Verbindungsanforderungsrichtlinie, die vier weiteren dann die Netzwerkrichtlinie. Also wie folgt:

"Wifi User Auth AD-Home"

Honome allovert	
Netzverkverbindungsm Wählen Sie den Typ de wird. Sie können entwe erfonterlich. Wenn der f angegeben" aus.	sthode 1 Natiowerkzugeffisservers aus, von dem die Verbindungsamfonderung an den Natiowerkrichtlinienserver gesendet die den Typ das Natiowerkzugeffisservers oder "Namsalampazitisch" auswählter, kanne dar backen Angaben ist jadoch ietzwerkzugeffisserver ein 802, 1XX-hattendflörerungsswitsth oder ein Diehttisszugeffisjunkt ist, wählen Sie "Nicht
Typ des Netzwerkzug	plfsserven:
Nicht angegeben	
Herstellerpezifisch:	
10 .	
renn de sædingungen o er Vietnindungsanforden	er versinsungsamonserung entspechen, vervencet set hezwenzotämenserer (14-10) die Hortene zum Aussissere ng. Wenn die Bedingungen der Verbindungserkorlerung nicht entsprechen, übergefingt der NPS diese Richtinis und
renn de secongunges o er Vietbindungsanforden ertet andere Richtlinien	er versindungsamssaming ensperionen, vervennet allt nedwenschamenarier (19-5) die Hichame aum Hutossene ng. Wenn die Bedingungen der Verbindungsanforderung nicht entgrechen, überspringt der NPS diese Richtinie und zus, fals verber Richtinen konfigurent and.
renn de tekongungen d er Verbindungsanforden ertet andere Richtlinien Bedingung	er versindungsamlickening antiperionen, versiennet aar neceleenordamenaaner (hurs) die nodame aum nubbieering ng. Ween die Sedingungen der Verbindungsanforderung nicht entigerechen, überspringt der NPS diese Richtlinie und zus, falls verbere Richtlinien konfiguriert sind.

Bedingungsbeschreibung: Die Bedingung "NAC-Pottijo" gibt den vom Zugtflictiert verwendeten Medientyp an, z.B. analoge Telefonietungen, ISDN, Tunnel oder VP IEEE 802.11 dahlde und Ethemet-Gwitzhes.

Erforderliche Authentifizierungsmethoden	Netzwerkrichtlinien-Authentifizierungseinstellungen außer Kraft setzen		
Authentifizierungsmethode	Anstelle der Einschvänkungen und Authentifizierungseinstellungen in der Netzwerksichtlinie werden diese Authentifizierungseinstellungen verwendet.		
Weiterleitungsverbindungsanfor derung			
Authentifizierung	EAD Turner supplies well chars Matrix and citized interaction and Clark in day		
Nontofährung	angezeigten Reihenfolge ausgehandelt.		
Bereichsname angeben	EAP-Typer:		
Atribut			
RADIUS-Attribute	Nach unten		
😝 Standard	Hinzufügen Bearbeiten Endernen		
I Herstellerspezifisch	Weniger sichere Authentitzierungsmethoden:		
	Microsoft-eerschüsselte Authentifizierung, Version 2 (MS-CHAP-42)		
	Benutzer darf das Kennwort nach Ablaufdatum ändem		
	Microsoft-verschlüsselte Authentifizierung (MS-CHAP)		
	Benutzer darf das Kennvort nach Ablaufdatum ändern		
	Verschlüsseite Authentifizierung (CHAP)		
	Unverschlüsselte Authentifizierung (PAP, SPAP)		

Richtlinienstatus

Falls aktiviert, wertet der Netzwerkschtlinienserver (NPS) diese Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus. Richtlinie aktiviert

Zupriffsbe

Zugefnbesechtigung Vielen die Bedingungen und Einschränkungen der Netzwerkrichtlinie der Verbindungsanforderung entsprechen, kann die Richtleise erholder den Zugniff gewähren oder verweigens. <u>Vien ist eine Zugnifisberschlaung?</u>

Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.

Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspricht.

Benutzerkonto-Enwähleigenschaften ignorieren

Umstandhund Erheitingentostenen geheren Wenn de Verbaungestrotstenen gan Bedingungen und Einschränkungen deser Netzwerkrichtlinie erhspicht und die Richtlinie den Zugiff gewähnt, wird die Ausniserung nur mit der Netzwerklichtlinie ausgeführt. Die Einwählegenschaften der Benutzerkonten werden mit dit ausgewentet.

Netzwerkverhindungsmethode Wälken Sie den Typ des Netzwerkzugliftserven aus, von dem die Vetändungsanforderung an den Netzwerkrähtlisienserver gesendet wird. Sie können eintweder den Typ des Netzwerkzugriftservens oder "Hestellerspectinch" auswählten, keine der beden Angaben ist jedoch efraudekdi. Wienn der Netzwerkzugriftserver ein 802. 1X-Authentfosierungsankon oder ein Disht/sazugitfispunkt at, wählen Sie "Nicht engegeben" wird.

Typ des Netzwerkzugriffsservers:

is (sonstige) OR Drahtlos (IEEE 802.11)	
ME/Grp-WLAN-AD-Home	

dren müs



"Wifi User Auth Iot"

Richtlinienstatus Esite sitti int usetat dari	
Early addition to send of days	
deaktiviert, wertet der NF	Netzwerkichtlinienserver (NPS) diese Richtlinie beim Verarbeiten der Verbindungsenforderungen aus. Fells 25 diese Richtlinie nicht aus.
Richtlinie aktiviert	
atzue (certindungune	foole
Wählen Sie den Typ des viel. Sie können entwed inforderlich. Wenn der N ingegeben" aus.	Netzwerkzugeffeanwer aus, von dem die Verbindungsenforderung en den Netzwerkschifteinenemer generotet in dem Trychen Netzwerkzugeffesteren oder "Hereitelingereford" ausschlehen, keiner der bestein Angelans ini jedoc stanwerkzugeffestenver ein 852. IX-Authentifizierungsswicht oder ein Dehtloszugeffepunkt ist, wehlen Sie "Nicht
Typ des Netzwerkzug	disservers.
Noht angegeben	w
Herstellerpezifisch:	
90 0	
nn cie beongungen or Verbindungsanforderu rtet andere Richtfinien o	er versinsburgsamstonerung entsprechen, vervenset ber nestweitvortismenserver parsy bei nichtene zum Austres ng. Wenn die Bedingungen der Verbindungsanfanderung nicht entsprechen. überspringt der NPS diese Richtlinie r zu, fels weitere Richtlinen konfiguiert sind.
Bedingung	Wert
NAS Portes	
	Drahtkos (sonatige) OR Drahtkas (IEEE 802.11)
dngungsbeschwebung	Chekhion (sonatige) OH Chekhies (IEEE 800.11)
dingungsbeschreibung Beleingung "NAG-Port	Deshfon (sonarige) OH Deshfos (EEE 800.11) yp" gibt den vom Zugeffsolient verwendeten Medievtyp an, z.B. analoge Telefonleitungen, ISDN, Tunnel oder VP Ethemet-Svitches.

Erforderliche Authentifizierungsmethoden	Netzwerkrichtlinien-Aufhentifizierungseinstellungen außer Kraft setzen		
Authentificierungsmethode	Anstelle der Einschlänkungen und Auftrentifizierungseinstellungen in der Netzwerkschlinie werden diese Aufterntifizierungseinstellungen verwendet.		
Weiterleitungsverbindungsanfor Serung			
Authentifizierung	FAD From conductor induced induction and that is down		
Nantolührung	angezeigten Rehenfolge ausgehandelt.		
Bereichoname angeben	EAP-T jperc		
Atribut	Nach ober		
ADIUS-Attribute	Nach unter		
Standard	Hinzufügen Bearbeiten Entlemen		
Herstellerspezifisch	Weniger sichere Authentifizierungsmethoden:		
	Microsoft-verschüsseite Authentifizierung, Version 2 (MS-CHAP-v2) Benutzer derf das Kennwort nach Ablaufdatum ändern		
	Microsoft-verschlüsseite Authentifizierung (MS-CHAP)		
	Benutzer darf das Kennwort nach Ablaufdatum ändem		
	Verschlüsselte Authentifizierung (CHAP)		
	Unverschlüsselte Authentifizierung (PAP, SPAP)		

Richtlinienstatus

Falls aktivient, wertet der Netzwerkrichtlinienserver (NPS) diese Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus.

Richtinie aktiviert

Zugriftsberechtigung Wenn die Bedingungen und Einschränkungen der Netzwerkrichtlinie der Verbindungsanforderung entsprechen, kann die Richtlinie entweder den Zugrift gewähren oder verweigern. <u>Was ist eine Zugriftsberechtigung:</u>

S Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.

2 Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspicht.

C Benutzerkonto-Einwähleigenschaften ignorieren

Unservationstructure annument generation of generation of the second sec

Netzwerkosteindungsmethode Wählen Sie den Try den Netzwerkzugriftsenven zus, von dem die Verbindungsanforderung an den Netzwerkohtliniensener gesendet wird Sie klosen entweder den Typ des Netzwerkzugriftsenven oder "Hentellengeziftsch" auswählen, keine der beiden Angeben ist pröch erforderlich, Wern der Netzwerkzugriftsenver en 602.1X-Auchentfolerungszwich oder ein Dehtissaugriftsportel ist, wählen Bie "NetN

Typ des Netzverkzugriffsservers:

	Bedingung	Viert
9	NAS-Portyp	Drahtlos (sonstiga) OR Drahtlos (IEEE 802.11)
Ù	Windows-Gruppe	INT-HOMEIGrp-WLAN-IoT

angehören müssen



https://ubiquiti-networks-forum.de/wiki/entry/106-vlan-zuweisung-und-wlan-registrierung-%C3%BCber-zertifikate-bzw-nutzername-mit-nps-9 <u>ra/</u>

"Wifi Device Cert Auth"

Richtinienstatus	
Falls aktiviert, wertet der	Netzwerkichtlinienserver (NPS) diese Richtlinie beim Verarbeiten der Verbindungsanforderungen aus. Falls
deaktiviert, wertet der Ni	15 diese Richtlinie nicht aus.
Richtlinie aktiviert	
Netzwerkverbindungsme	Diade
Wählen Sie den Typ des wird. Sie können entwed erforderlich. Wenn der N angegeben" aus.	Netzwerkzugefflaserver aus, von dem die Varbindungsantodarung an den Netzwerkräftlieienswer gesendet er den Try des Netzwerkzugriffeserves oder "Neterlationspecificht" zwerklier, leiner der beiden Angeben ei uplach stzwerkzugefflaserver ein 822.1X-Auftentflaserungsanktich oder ein Drahtbazugefflapunkt at, wählen Sie "Nicht
Typ des Netzwerkzug	ifisiervers.
Noht angegeben	w
O Herstellerpezifisch:	
wenn die secongungen de	r verbindungsantorderung entsprechen, verwendet der Netzwenkontzinnenserver (no-to) die Hochtine zum Hubbiseer
der Verbindungsenforderu	g. Wenn die Bedingungen der Verbindungsanfanderung nicht entsprechen, überspringt der NPS diese Richtlinie und
wertet andere Richtlinien a	u.s. falls welsen Richtlinie konfiguret istid.
wenn die secongungen de	r verbindungsantstreeung einsprechen, verwendet zer treizweinschaftenzeinenzener portig die rochsine zum vuossene
der Verbindungsenforderu	ng. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPG diese Richtlinie und
werket andere Richtlinien a	us, talls weitene Richtlinien konfiguriet sind.
wenn die secongungen or	r verbindungsantsroeeung entsprechen, vervendet zer hestwenschatenserver por-toj die rochtene zum rubbseer
der Verbindungsanforderu	rg. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPS diese Richtlinie und
verbet andere Richtlinien a	us, talls verlane Richtlinien konfiguriet sind.
Bedingung	Weit
venn die secongungen od	r Verbindungsanstraterung entsprechen, verwendet der Netzwenkransenserver pro-toj die Honterue zum Hucossere
der Verbindungsenfonteru	rg. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPG diese Richtlinie und
wertet andere Richtlinien s	us, falls weitere Richtlinien konfigurient sind.
Bedingung	Went
NAS-Porsyp	Dishridus (IEEE 802 11) OR Diternet OR Drahfos (scrutige)
venn de tekorgungen og	r verbnoungsantorsening entsprechen, verwendet bet Netwenkrichsenserver pe-bij die Hontene zum Hudossere
Verkindungserforderu	rg. Wenn die Bedingungen der Verbindungsanfordening nicht entsprechen, überspringt der NPS diese Richtlinie und
vertet andere Richtinien a	us, tals weitere Richtlinien konfiguriet sind.
Bedingung	Weit
Bedingung	Drafelde (EEEE 802 11) OR Enternet OR Drafeldes (sonstige)
wenn de sekongungen o	r verbnoungsantorseung entsprechen, verwendet det Netwenschnenssever pe-by die Hontene zum Automeere
der Verbindungserforderu	rg. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPS diese Richtlinie und
wertet andere Richtlinien a	us, tals weiten Richtlinien konfiguriet sind.
Bedingung	Weit
WASS-Plorzyp	Drafelde (EEEE 802.11) OR Erbennet OR Drafelde (sonstige)
wenn de sekongungen o	r verbnoungsantorsenung entsprechen, verwendet bet Nettwenschnenssever per-bij die Hontene zum Automeere
der Verbindungsenforderu	rg. Wenn die Bedingungen der Verbindungsanfordenung nicht entsprechen, überspringt der NPS diese Richtlinie und
wertet andere Richtlinien a	us, tals weitere Richtlinien konfiguriet sind.
Bedingung	Wen:
RASS-Purzyp	Dranklas (IEEE 802 11) DR Enterwet DR Drahklas (sonstige)
wenn de seongungen o	er vertonoungeantorcenung entoprechen, verwendet ber Netzwenkorcheneberver po-toj die Honterne zum Huddiseere
der Verbindungsenforderu	ng. Wenn die Bedingungen der Verbindungsanforderung nicht entoprechen, überspringt der NPG diese Richtlinie und
wertet andere Richtlinen a	us, talls weitere Richtlinien konfigurient sind.
Bedingung	Went
NAS-Pureyp	Drahtlas (IEEE 802 11) OR Ditternet OR Drahtlas (sonatige)
wenn de tekongungen od der Verbindungsenforderu wertet andere Richtlinien a Bedingung Bedingung MAG-Portyp	r Vetonoungeanstreaung enterpresien, verwendet der Netoversnortsneeterver pro-tig die Honterne zum Husonseen ng. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPG diese Richtlinie und us, falls weitere Richtlinien konfigurieit sind. Went Distribus (IEEE 202 11) OR Etherwet OR Drahtlos (sonatige)
vven de seongungen o	r vetonoungeantoteeung entoprechen, verwencet oer Netovennortsneetserver pe-tig de NPR diese Richtline und
der Verbindungserforderu	ng. Wenn die Bedingungen der Verbindungsanforderung nicht entoprechen, überspringt der NPR diese Richtline und
wertet andere Flichtlinien s	us, falls weitere Richtlinen konfigurieit sind.
Bedingung	Went
Statisticker	Debriste (ISSE 2022-11) OR Ethernet OR Drahfwa (sonatige)
wenn de sekongungen o	r veronoungeantorseung entoprechen, verwendet det Netwentorstanenseiver (ne-to) die Hothere zum Huddiseere
der Verbindungsenfonteru	ng. Wenn die Bedrigungen der Verbindungsanforderung nicht entoprechen, überspringt der NPG diese Richtlinie und
wertet andere Richtlinten s	us, falls weiten Richtlinien konfigurief sind.
Bedingung	Weit
Bedingung	Drahtles (EEEE 602:11) OR Different OR Drahtlos (sonstige)
wenn de sekongungen o	r verbnoungeantarsenung enteprechen, verwendet bet Nettwentarsteinessever (no-50 die Nortenie zum Automeer
der Verbindungsenfonderu	rg. Wenn die Bedingungen der Verbindungsanfordenung nicht entsprechen, überspringt der NPG diese Richtlinie und
wertet andere Richtlinien a	us, tals weitere Richtlinien konfigurieit sind.
Bedingung	Wen:
WASS-Plorzyp	Dranklas (IEEE 802 11) DR Enternet OR Drahklas (sonstige)
wenn de seongungen o der Verbindungsenforderu wentet andere Richtlinten a Bedingung RAS-Ruszyp Bedingungsbeschreibung Bedingungsbeschreibung	r vetonoungeantaneung entepresten, venvencet ser Netwentvorsneetsever po-toj de Honterne zum Autoneere gi, Wenn die Bedingungen der Verbindungsanfordenung nicht entspenchen, überspringt der NPG diese Richtlinie und us, tals weitere Richtlinien konfigurient sind. Went Drahtlas (IEEE 802 11) OR Diternet OR Drahtlas (sonatige)



Richtlinienstatus Falls aktiviet, werter der Netzwerklichtlinienserver (NPG) dess Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet de NPG diese Richtlinie nicht aus.

Richtlinie aktiviert

Zugriffs

Zugritsbewichtigung Vrienn die Bedingungen und Einschränkungen der Netzwerknichtlinie der Verbindungsanforderung entsprechen, kann die Richtlinie entweder den Zugriff gewähren oder verweigen. <u>Vrien ist eine Zugriffsberechtigung?</u>

Szupiff gewähren. Der Zupiff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.

Zugiff verweigen. Der Zugiff wird verweigen, wenn die Verbindungsanforderung dieser Richtlinie entspricht.

Benutzerkonto Einvelhleigenschaften ignorieren
Wenn die Verlindungsamthotierung den Bedingungen und Einschränkungen dieser Netzwerkrichtlinie entspricht und die Richtlinie den
Zugeff genählt, wird die Autorisierung nur mit der Netzwerkrichtlinie ausgeführt. Die Einvelhleigenschaften der Benutzerkonten werden
nicht ausgewartet.

rbindungsmethode

Wählen Sie den Typ des Netzwerkzugilfisienens aus, von den die Verbindungsenforderung an den Netzwerkinhfiniensener gesendet wird. Ein können entweder den Typ des Netzwerkzugilfisienens oder "Hensellenpezifisch" auswähler, keine der beiden Angeben ist jedoch effordende. Winn der Netzwerkzugilfisienen ein 602.1X-Auftenficierungsweiten oder ein Diehtloszugilfispunkt ist, wählen Sie Trächt angegeben" zur

Typ des Netzwerkzugriffsse

Nicht angegeben Wen die Bedingungen der Verbindungsanfordenung entsprechen, verwendel der Netzwerkichtlinienserver die Richtlinie zum Autorisieren der Verbindungsanforderung. Wen die Bedingungen der Verbindungsantorderung nicht entsprechen, überspringt der Netzwerkichtlinienserver diese Richtlinie und vertet andere Richtlinien aus, falls weitere Richtlinien konfiguriert sind.

Bedingung	Wet
Computergruppen	INT-HOME/Orp-WanDavices OR INT-HOME/Orp-LanDavices
gungsbeschreibung:	
edingung "Computerge	ppen" gibt an, dass der Computer, der eine Verbindung hersteilt, zu einer der ausgewählten Gruppen gehörer

Enschränkungen: Einschtäskungen Autentifizierungsmethode Zugriff nur für Clients gewähren, die sich mit den angegebenen Methoden authentifizieren. 1 Leerlaufzeitüberschreitung EAP-Typen werden zwischen Netzwerkrichtlinienserver und Client in der angezeigten Rehenfolge ausgehandeit. 🛐 Sitzungszeitüberschreitung EAP-Typen: 🛅 Emplangs-ID Nach oben Microsoft: Smartcard- oder anderes Zertifikat Tag- und Uhrzeiteinschränkungen Nach unten T NAS-Portyp ε 3 Hinzufügen... Bearbeiten... Entfernen Weniger sichers Aufhentifizierungsmethoden: Microsoft-verschlüsseite Authentifizierung, Version 2 (MS-CHAP-v2) Benutzer derf das Kennwort nach Ablaufdatum ände Microsoft-verschlüsselte Authentifizierung (MS-CHAP) Benutzer derf das Kennwort nach Ableufdetum ändern Verschlüsselte Authentifizierung (CHAP) Unverschlüsselte Authentifizierung (PAP, SPAP) Clentverbindungen ohne Aushandlung einer Aufhentifizierungsmethode zulassen Einstellungen: RADIUS-Attribute Wählen Sie ein RADIUS-Grandendstribut aus, und kloken Sie dann auf "Beathelten", um zusätzliche Atholute an RADIUS-Clientz zu senden. Wenn Sie kein Atholut konfigurieren, wid kein Atalout an RADIUS-Clientz gesendet. Informationen zu den erfunderlichen Atholuten Inform Sie in der RADIUS-Clientzduurmentarion. Z Herstellerspezifisch Reating and RAS Mehrfachverbindung und BAP (Bandwidth Allocation-Protokoll) Attributer Nemo Wet T IP-Filter Framed-Protocol ppp Service-Type Framed Verschlüsselung Seniole-Type Finances Tunnei-Medium-Type 852 (includes all 802 media plus Ethemet canonical for.-Tunnei-P-Gauge-D 10 Tunnei-Type Visual LANs (vLAN) 💑 IP-Einstellungen Hinzufügen... Dearbeiten... Entfernen

https://ubiquiti-networks-forum.de/wiki/entry/106-vlan-zuweisung-und-wlan-registrierung-%C3%BCber-zertifikate-bzw-nutzername-mit-nps-<u>ra/</u> 11

4 Konfigurieren Unifi-Controller

am Beispiel der UDM-Pro (sollte jedoch auf allen anderen Instanzen wie Cloudkey etc. sehr ähnlich funktionieren)

Wechselt zu Netzwerk - Einstellungen - Profile - RADIUS - Create New RADIUS Profile

Einstellungen wie folgt:

"RADIUS Assigned VLAN Support" beide Haken setzen, sowohl Wired als auch Wireless

"RADIUS Settings"

Authentication Server: IP eures NPS eingeben und auch den gemeinsamen Schlüssel aus Punkt 4. Bei Port tragt ihr Port Nummer 1812 ein.

Haken setzen bei "enable Accounting" (ist nicht erforderlich, jedoch hilft es ungemein beim debugging)

Dieselben Daten eingeben wie bei Authentication Server, mit Ausnahme vom Port, hier tragt ihr diesmal Port Nummer 1813 ein.

Wired Networks 🕕	🕑 Enable				
Wireless Networks ()	🕑 Enable				
RADIUS Settings					
Authentication Servers		1812			🕀 Add
	IP ADORESS	PORT	SHARED SEC	RET	🥒 Edit
		1812			
Enable Accounting	📴 Enable				
RADIUS Accounting Servers	IP Address	1813		Shared Secrel	🕀 Add

Dann geht ihr zu Netzwerk - Einstellungen - Profile - Switch Ports - Create new profile



Einstellungen - Netzwerke

DHCP Snooping	🕝 Enable
Jumbo Frames (1)	Enable
Flow Control 🕕	Enable
Spanning Tree 🕕	○ STP
802.1X Control 🕕	🕝 Enable
RADIUS Profile	AD-NPS ~

Solltet ihr einen oder mehrer Switche nicht über die globalen Netzwerk-Einstellungen verwalten, so findet ihr die nötigen Schalter unter Unifi-Devices - "euer switch" - Settings - Services

Spanning Tree	
RSTP	
Priority	
32768	
802.1X Control (i)	

Einstellungen - WiFi

neue SSID mit Einstellungen aus dem Screenshot.

Advanced Configuration	Auto (Manual)
WiFi Band	🗧 2.4 GHz 👩 5 GHz 🕕
WiFi Type	Standard Guent Hotapot
Band Steering ()	🗧 Enable
Bandwidth Profile 🕕	Default ~
Multicast Management	
Client Device Isolation ()	🕞 Enable
Proxy ARP ()	Enable
RADIUS Profile	AD-NPS
PMF 🕕	C Required C Optional Disabled
Group Rekey Interval 🕕	Enable
Hide WiFi Name	C Enable
Device Filtering	
MAC Address Filter (1)	Enable
RADIUS MAC Authentication ()	Enable

Natürlich müsst ihr noch alle Switchports, bei denen das Profil "AD-NPS" verwendet werden soll, entsprechend konfigurieren.

Unifi-Devices - "euer switch" - portmangement

Warum auch immer muss man hier Netzwerk angeben, gleich der zweite Punkt. Es ist vollkommen egal, welches VLAN ihr hier eintragt, da es ignoriert wird. Sollte eure Authentifizierung am NPS fehlschlagen, rutschen eure Geräte automatisch in das Fallback-VLAN, das ihr bei "Global Switch Settings" eingegeben habt. Vielleicht bessert Ubiquiti hier ja irgendwann mal noch nach, damit das weniger verwirrend ist.

Das wars auch schon im Unifi-Controller.

5 Lan-fähige Windows Clients konfigurieren (bei Wifi-only Clients nicht nötig)

Windows-Suche - "Dienste"

Findet den Dienst dot3svc (Wired AutoConfig, deutsch: Automatische Konfiguration (verkabelt)). Dieser muss gestartet sein und auch beim Hochfahren automatisch starten.

Description:	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current			
Path to executab C:\Windows\sys	le: tem32\svchost.exe	+ LocalSystemNetw	ork Restricted -p	
Startup type:	Automatic			
Service status:	Running			
Start	Stop	Pause	Resume	

Wechselt nun zu den Netzwerkverbindungen. Rechtsklick auf euren Netzwerkadapter und dann Eigenschaften. Wechselt zum Reiter "Authentifizierung". Einstellungen wie in den Screenshots.



Bevor ihr scharf-schaltet, sollten alle Clients und alle Server gpupdate /force ausgeführt haben und einmal neu gestartet werden, damit auch alles GPOs übernommen wurden. Dies ist wichtig, damit die Clients die entsprechenden Zertifikatsanforderungen an die CA stellen.

6 Ergebnis

1. Nun sollten Nutzer, welche sich mit Ihrem Nutzernamen u. Passwort am WLAN anmelden in VLAN 10 eingewählt werden.

2. Der/die Nutzer der Gruppe IoT wählen sich in VLAN 16 ein

3. Laptops, die sich über WLAN verbinden und der Active Directory verbinden sich bereits vor der Nutzeranmeldung mit dem WLAN AD-Home und wählen sich im VLAN 10 ein

4. PCs, die der Active Directory angehören, werden, sobald sie mit einem Switch verbunden werden, in VLAN 10 eingewählt.

Wichtig:

für Server empfehle ich das Ganze ausdrücklich NICHT, da bei einer Fehlkonfiguration ein Aussperren aus den eigenen Systemen nicht ausgeschlossen werden kann.

Sollte ich irgendwo etwas vergessen haben zu erwähnen, nehmt es mir nicht übel, war doch alles etwas viel auf einmal zu schreiben. Weist mich einfach darauf hin, dann schau ich nochmal drüber.

Bekannte Bugs/Bugfixes:

- 1. Sollten eure RADIUS-Clients (Switches/Accesspoints) Schwierigkeiten haben, mit dem NPS zu kommunizieren, erstellt auf dem NPS bitte eine eingehende Firewallregel, in der ihr die Ports 1812 und 1813 erlaubt. Es besteht zwar eine solche Regel, jedoch wird sie aus welchen Gründen auch immer ignoriert. Dies ist ein bekannter Bug, der von MS auch schon bestätigt wurde.
- 2. Die Log-Files vom NPS lassen sich leider nicht auf einer Netzwerkfreigabe speichern. Workaround: ein Skript erstellen, welches die Dateien auf eine Freigabe synchronisiert.

Grüße aus BW und viel Erfolg beim Umsetzen!

Disclaimer:

dies ist nur eine grobe Anleitung. Ich bin weder auf diesem Gebiet geschult, noch kenne ich mich mit möglichen Sicherheitsrisiken aus. Alles was ihr tut, geschieht auf Eure eigene Verantwortung.

– Auswählen: -

Gültige Software-Version Keine Firmware-Relevanz!